

CLAIM LISTING

Kindly amend claims 1, 9-10, 16, and 21 as shown in the following listing of claims. The listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently Amended) An apparatus for performing cryptographic operations, comprising:
 - an x86-compatible microprocessor, comprising:
 - fetch logic, configured to receive a single, atomic cryptographic instruction, wherein said single, atomic cryptographic instruction is one of the instructions in an application program, wherein said application program is executed by said x86-compatible microprocessor, and wherein said single, atomic cryptographic instruction prescribes an encryption operation, and wherein said single, atomic cryptographic instruction prescribes one of a plurality of cryptographic algorithms;
 - algorithm logic, operatively coupled to said single, atomic cryptographic instruction, configured to direct said x86-compatible microprocessor to execute said encryption operation according to said one of a plurality of cryptographic algorithms; and
 - execution logic, operatively coupled to said algorithm logic, configured to execute said ~~one of the cryptographic~~encryption operation~~operations~~, wherein said execution logic ~~comprises~~comprises:
 - a cryptography unit for executing a plurality of cryptographic rounds required to complete said encryption operation, wherein said cryptography unit executes a first plurality of micro instructions generated by translation of said single, atomic cryptographic instruction; and

an x86 integer unit, wherein said cryptography unit operates in parallel with said x86 integer unit to accomplish said encryption operation, and wherein said x86 integer unit executes a second plurality of micro instructions generated by translation of said single, atomic cryptographic instruction to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said encryption operation.

2. (Previously Presented) The apparatus as recited in claim 1, wherein said encryption operation comprises encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.
3. (Previously Presented) The apparatus as recited in claim 1, wherein the cryptographic operations comprise:

a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.
4. (Original) The apparatus as recited in claim 1, wherein said one of a plurality of cryptographic algorithms comprises the Advanced Encryption Standard (AES) algorithm.
5. (Original) The apparatus as recited in claim 1, wherein said one of a plurality of cryptographic algorithms comprises the Digital Encryption Standard (DES) algorithm.
6. (Original) The apparatus as recited in claim 1, wherein said one of a plurality of cryptographic algorithms comprises the Triple-DES algorithm.
7. (Previously Presented) The apparatus as recited in claim 1, wherein said single, atomic cryptographic instruction is prescribed according to the x86 instruction format.

8. (Previously Presented) The apparatus as recited in claim 1, wherein said single, atomic cryptographic instruction implicitly references a plurality of registers within said x86-compatible microprocessor.
9. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:
 - a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks upon which said encryption operation is to be accomplished, and wherein said first register comprises one of said text pointer registers.
10. (Currently Amended) The apparatus as recited in claim 8, wherein said plurality of registers comprises:
 - a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said encryption operation upon a plurality of input text blocks, and wherein said second register comprises one of said text pointer registers.
11. (Original) The apparatus as recited in claim 8, wherein said plurality of registers comprises:
 - a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

12. (Previously Presented) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said encryption operation.

13. (Previously Presented) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said encryption operation.

14. (Previously Presented) The apparatus as recited in claim 8, wherein said plurality of registers comprises:

a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said encryption operation.

15. (Previously Presented) The apparatus as recited in claim 1, wherein said cryptography unit executes said plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, and wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit.

16. (Currently Amended) An apparatus for performing cryptographic operations, comprising:

an x86-compatible microprocessor, comprising:

a cryptography unit, configured to execute a decryption operation responsive to receipt of a single, atomic cryptographic instruction that prescribes said decryption operation, wherein said single, atomic cryptographic instruction is one of the instructions in an application program that are fetched from memory by fetch logic in said x86-compatible microprocessor, and wherein said x86-compatible microprocessor executes said application program, and wherein said cryptography unit executes a first plurality of micro instructions generated by translation of said single, atomic cryptographic instruction, and wherein said single, atomic cryptographic instruction comprises:

an algorithm field, configured to prescribe one of a plurality of cryptographic algorithms to be employed when executing said decryption operation; and

an x86 integer unit, wherein said cryptography unit operates in parallel with said x86 integer unit to accomplish said decryption operation, and wherein said x86 integer unit executes a second plurality of micro instructions generated by translation of said single, atomic cryptographic instruction to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said decryption operation; and

algorithm logic, operatively coupled to said cryptography unit, configured to direct said x86-compatible microprocessor to perform said decryption operation according to said one of the plurality of cryptographic algorithms.

17. (Original) The apparatus as recited in claim 16, wherein said one of a plurality of cryptographic algorithms comprises the Advanced Encryption Standard (AES) algorithm.
18. (Original) The apparatus as recited in claim 16, wherein said one of a plurality of cryptographic algorithms comprises the Digital Encryption Standard (DES) algorithm.
19. (Original) The apparatus as recited in claim 16, wherein said one of a plurality of cryptographic algorithms comprises the Triple-DES algorithm.
20. (Previously Presented) The apparatus as recited in claim 16, wherein said single, atomic cryptographic instruction is prescribed according to the x86 instruction format.
21. (Currently Amended) A method for performing cryptographic operations, comprising:

fetching a single, atomic cryptographic instruction for execution by an x86-compatible microprocessor, wherein the single, atomic cryptographic instruction prescribes an encryption operation and one of a plurality of cryptographic algorithms

translating the single, atomic cryptographic instruction into a first plurality of micro instructions and a second plurality of micro instructions; and

via a cryptography unit and an x86 integer unit operating in parallel in the x86-compatible microprocessor, ~~executing~~performing the encryption operation according to the one of the cryptographic algorithms, said performing comprising:

first executing the first plurality of micro instructions within the cryptography unit to perform a prescribed number of cryptographic rounds to produce a block of output data; and

second executing the second plurality of micro instructions within the x86 integer unit in parallel with said first executing to test a bit in a flags register, to update text pointer registers, and to process interrupts during execution of said decryption operation.

22. (Original) The method as recited in claim 21, wherein the one of a plurality of cryptographic algorithms comprises the Advanced Encryption Standard (AES) algorithm.
23. (Original) The method as recited in claim 21, wherein the one of a plurality of cryptographic algorithms comprises the Digital Encryption Standard (DES) algorithm.
24. (Original) The method as recited in claim 21, wherein the one of a plurality of cryptographic algorithms comprises the Triple-DES algorithm.
25. (Previously Presented) The method as recited in claim 21, wherein said fetching comprises:

prescribing the single, atomic cryptographic instruction according to the x86 instruction format.